CC and CMMI®

An Approach to Integrate CC with Development

Wolfgang Peter
Contents

1. Status Quo
2. CMMI® for Development
3. Striking Analogies
4. Combining Standards
5. Conclusion
What CC does accomplish ...

- assesses and rates security capabilities of IT products
- establishes various levels of confidence in those products
- offers flexibility for new type of products and configurations, and development models
- provides mutual recognition, i.e. dozens of countries and many commercial users buy into working with CC
- ...
... but ...

Ø uses a complex and somehow artificial “language” developers are not familiar with

Ø usually starts fairly late in the development process

Ø requires documents “just for CC”

Ø focuses on product features, not on development processes

Ø ...
Bottom line

- CC is normally not integrated with development
- CC causes disruption from regular development processes
- CC often results in established coexistences of “normal” and “CC development” within organizations
- CC is typically not institutionalized within an organization
Associated risks

- CC is normally not integrated with development
- Decisions on a case by case basis
- CC causes disruption from regular development processes
- Unnecessary “overhead” Waste of time and money
- CC often results in established coexistences of “normal” and “CC development” within organizations
- No efficient re-usage of development results (specifications, test results, development documents etc.)
- CC is typically not institutionalized within an organization
- Heavy dependent on individuals No guarantees that historical results can be repeated
In general ...

- The quality of a product is highly influenced by the quality of the processes used to acquire, develop, and maintain it.

- Every organization involved in the development of security products would basically benefit from experiences and best-practices of well-defined and structured engineering standards.

Source: SEI, Mastering Process Improvement
Contents

1. Status Quo
2. CMMI® for Development
3. Striking Analogies
4. Combining Standards
5. Conclusion
Background

- **CMMI® (Capability Maturity Model® Integration)** is a process improvement approach that provides organizations with the essential elements of effective processes.

- Successor of CMM or Software CMM; CMM developed from 1987 through 1997; release of CMMI, V1.1 in 2002.

- Created by members of industry, government and the SEI (Software Engineering Institute, Pittsburgh, PA, USA).

- Three models:
  - **CMMI for Development** (CMMI-DEV), Version 1.2 (08/2006)
  - **CMMI for Acquisition** (CMMI-ACQ), Version 1.2 (11/2007)
  - **CMMI for Services** (CMMI-SVC), (2009)

- Primary focus: process improvement
  - Organizations cannot be CMMI “certified”, but are appraised and awarded a 1-5 level rating (e.g., using **SCAMPI - Standard CMMI Appraisal Method for Process Improvement**).

- Web Site: [http://www.sei.cmu.edu/cmmi/](http://www.sei.cmu.edu/cmmi/)
Key concept

- **Process**
  - sequence of steps performed for a given purpose

- **Process Areas (PA)**
  - characteristics of effective processes

- **Specific/Generic Goals (SG/GG)**
  - requirements

- **Specific/Generic Practices (SP/GP)**
  - expected activities

- **2 types of representations**
  - continuous
  - staged

- **Capability Level (CL)**
  - CL 0, CL 1, ..., CL5 (cumulative)
  - PA specific
  - CL i = achievement of GG i in a PA

- **Maturity Level (ML)**
  - ML 1, ML 2, ..., ML 5 (cumulative)
  - pre-defined set of PAs, each reaching a pre-defined CL
Continuous representation: Process Areas by categories - 1
### Continuous representation: Process Areas by categories - 2

<table>
<thead>
<tr>
<th>Process Management</th>
<th>Project Management</th>
<th>Support</th>
<th>Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPF</td>
<td>PP</td>
<td>CM</td>
<td>REQM</td>
</tr>
<tr>
<td>OPD</td>
<td>PMC</td>
<td>PPQA</td>
<td>RD</td>
</tr>
<tr>
<td>OT</td>
<td>SAM</td>
<td>MA</td>
<td>TS</td>
</tr>
<tr>
<td>OPP</td>
<td>IPM</td>
<td>DAR</td>
<td>PI</td>
</tr>
<tr>
<td>OID</td>
<td>RSKM</td>
<td>QPM</td>
<td>VER</td>
</tr>
</tbody>
</table>

- **Project Management**
  - PP: Project Planning
  - PMC: Project Monitoring and Control
  - SAM: Supplier Agreement Management
  - IPM: Integrated Project Management
  - RSKM: Risk Management
  - QPM: Quantitative Project Management

- **Process Management**
  - OPF: Organizational Process Focus
  - OPD: Organizational Process Definition
  - OT: Organizational Training
  - OPP: Organizational Process Performance
  - OID: Organizational Innovation and Deployment

- **Support**
  - CM: Configuration Management
  - PPQA: Process and Product Quality Assurance
  - MA: Measurement and Analysis
  - DAR: Decision Analysis and Resolution
  - CAR: Causal Analysis and Resolution

- **Engineering**
  - REQM: Requirements Management
  - RD: Requirements Development
  - TS: Technical Solution
  - PI: Product Integration
  - VER: Verification
  - VAL: Validation
Generic Goals 1-3

GG 1 Achieve Specific Goals
   GP 1.1 Perform Specific Practices

GG 2 Institutionalize a Managed Process
   GP 2.1 Establish an Organizational Policy
   GP 2.2 Plan the Process
   GP 2.3 Provide Resources
   GP 2.4 Assign Responsibility
   GP 2.5 Train People
   GP 2.6 Manage Configurations
   GP 2.7 Identify and Involve Relevant Stakeholders
   GP 2.8 Monitor and Control the Process
   GP 2.9 Objectively Evaluate Adherence
   GP 2.10 Review Status with Higher Level Management

GG 3 Institutionalize a Defined Process
   GP 3.1 Establish a Defined Process
   GP 3.2 Collect Improvement Information
### Staged representation: Process Areas by Maturity Level

<table>
<thead>
<tr>
<th>Generic Goal / Capability Level</th>
<th>ML 1</th>
<th>ML 2</th>
<th>ML 3</th>
<th>ML 4</th>
<th>ML 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organizational Innovation and Deployment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Optimizing</strong></td>
</tr>
<tr>
<td><strong>Causal Analysis and Resolution</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Quantitatively Managed</strong></td>
</tr>
<tr>
<td><strong>Organizational Process Performance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Quantitatively Managed</strong></td>
</tr>
<tr>
<td><strong>Organizational Process Focus</strong></td>
<td></td>
<td></td>
<td><strong>Defined</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organizational Process Definition + IPPD</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Organizational Training</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrated Project Management + IPPD</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Decision Analysis and Resolution</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Requirements Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td><strong>Project Planning</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td><strong>Project Monitoring and Control</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td><strong>Supplier Agreement Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td><strong>Measurement and Analysis</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td><strong>Process and Product Quality Assurance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
<tr>
<td><strong>Configuration Management</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Managed</strong></td>
</tr>
</tbody>
</table>

Source: method park, 2008
Contents

1. Status Quo
2. CMMI® for Development
3. Striking Analogies
4. Combining Standards
5. Conclusion
# Look and see!

## Organizational Innovation and Deployment
- Causal Analysis and Resolution

## Organizational Process
- Performance
- Quantitative Project Management

## Requirements Development
- Technical Solution
- Product Integration
- Verification
- Validation
- Organizational Process Focus
- Organizational Process Definition +IPPD

## Organizational Training
- Integrated Project Management +IPPD
- Risk Management
- Decision Analysis and Resolution

## Requirements Management
- Project Planning
- Project Monitoring and Control
- Supplier Agreement Management
- Measurement and Analysis
- Process and Product Quality Assurance
- Configuration Management

### Generic Goal / Capability Level

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
</table>

### Plus Critical Subprocesses

<table>
<thead>
<tr>
<th>Assurance class</th>
<th>Assurance Family</th>
<th>Assurance Components by Evaluation Assurance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development</td>
<td>ADV ARC</td>
<td>EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7</td>
</tr>
<tr>
<td>Development</td>
<td>ADV FSP</td>
<td>1 2 3 4 5 6</td>
</tr>
<tr>
<td>Development</td>
<td>ADV IMP</td>
<td>1 1 2 2</td>
</tr>
<tr>
<td>Development</td>
<td>ADV INT</td>
<td>2 3 3</td>
</tr>
<tr>
<td>Development</td>
<td>ADV SPM</td>
<td>1</td>
</tr>
<tr>
<td>Development</td>
<td>ADV TDS</td>
<td>1 2 3 4 5 6</td>
</tr>
<tr>
<td>Guidance documents</td>
<td>AGD OPE</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Guidance documents</td>
<td>AGD PDE</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC CMC</td>
<td>1 2 3 4 5 5</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC CMS</td>
<td>1 2 3 4 5 5</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC DEL</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC DVS</td>
<td>1</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC FDL</td>
<td>1 1 2 2</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC LTD</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Life-cycle support</td>
<td>ALC TAT</td>
<td>1 2 3 3</td>
</tr>
<tr>
<td>Security Target evaluation</td>
<td>ASE CCL</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Security Target evaluation</td>
<td>ASE ECD</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Security Target evaluation</td>
<td>ASE INT</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Security Target evaluation</td>
<td>ASE OBI</td>
<td>1 2 2 2</td>
</tr>
<tr>
<td>Security Target evaluation</td>
<td>ASE REO</td>
<td>1 2 2 2</td>
</tr>
<tr>
<td>Security Target evaluation</td>
<td>ASE SPD</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Security Target evaluation</td>
<td>ASE TSS</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Tests</td>
<td>ATE COV</td>
<td>1 2 2 2</td>
</tr>
<tr>
<td>Tests</td>
<td>ATE DPT</td>
<td>1 2 3 3</td>
</tr>
<tr>
<td>Tests</td>
<td>ATE FUN</td>
<td>1 1 1 1</td>
</tr>
<tr>
<td>Tests</td>
<td>ATE IND</td>
<td>1 2 2 2</td>
</tr>
<tr>
<td>Vulnerability assessment</td>
<td>AVA VAN</td>
<td>1 2 2 2 3 4 5 5</td>
</tr>
</tbody>
</table>
Analogy of key terms

- Process Area
- PA Category
- Capability Level
- Maturity Level
- Addition
- Assurance Family
- Assurance Class
- Assurance Component Leveling
- EAL
- Extension

*Both, CMMI and CC, represent state of the art concepts and culmination of decades of experiences*
Contents

1. Status Quo
2. CMMI® for Development
3. Striking Analogies
4. Combining Standards
5. Conclusion
An organization develops products with different requirements on functionality, security, and ... (e.g. safety)

Process Areas of CMMI-DEV cover demands on planned and controllable product development

CC covers additional security related requirements, for the product and the product’s development environment

... (e.g. IEC 61508)
Example: ALC_CMS (CM Scope)

**Configuration Management**

**Generic Goals & Practices**

**GG 1 Achieve Specific Goal**
- GP 1.1 Perform Specific Practices

**GG 2 Institutionalize a Managed Process**
- GP 2.1 Establish an Organizational Policy
- GP 2.2 Plan the Process
- GP 2.3 Provide Resources
- GP 2.4 Assign Responsibility
- GP 2.5 Train People
- GP 2.6 Manage Configurations
- GP 2.7 Identify and Involve Relevant Stakeholders
- GP 2.8 Monitor and Control the Process
- GP 2.9 Objectively Evaluate Adherence
- GP 2.10 Review Status with Higher Level Management

**GG 3 Institutionalize a Defined Process**
- GP 3.1 Establish a Defined Process
- GP 3.2 Collect Improvement Information

**Specific Goals & Practices**

**SG 1 Establish Baselines**
- SP 1.1 Identify Configuration Items
- SP 1.2 Establish a Configuration Management System
- SP 1.3 Create or Release Baselines

**SG 2 Track and Control Changes**
- SP 2.1 Track Change Requests
- SP 2.2 Control Configuration Items

**SG 3 Establish Integrity**
- SP 3.1 Establish Configuration Management Records
- SP 3.2 Perform Configuration Audits

**ALC_CMS.4: Problem tracking CM coverage**

**ALC_CMS.4.1C** The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; and security flaw reports and resolution status.

**ALC_CMS.4.2C** The configuration list shall uniquely identify the configuration items.

**ALC_CMS.4.3C** For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

**CC EAL4 specific requirements**

Institutionalization of this PA within the organization

Achievement of process related requirements
Activities and (first) results

- Focused on EAL4
- Bi-directional “mapping” and parts of the integration CC/CMMI-DEV done
- EAL4 does not require any addition of new CMMI-DEV process areas
- CMMI-DEV specific goal needs to be added (‡ ALC_DVS)
- Lots of additions to specific practices in engineering, project management, and support will be needed
- Lots of additions to the CMMI-DEV informative material necessary
Contents

1. Status Quo
2. CMMI® for Development
3. Striking Analogies
4. Combining Standards
5. Conclusion
Conclusion and next steps

- Experience shows that efficiently developing high quality/security products requires managing the engineering processes.
- In this respect CC needs to evolve or be combined with engineering standards.
- Combining CMMI-DEV and CC is feasible.
  - e.g. EAL4 would require Capability Level 3 of quite a few CMMI Process Areas.
- Piloting with customers will follow.
- Models will be implemented in a web based tool, supporting:
  - reference models
  - process definition
  - management.